Parametrization of the box variety by theta functions

Eberhard Freitag
Mathematisches Institut
Im Neuenheimer Feld 288
D69120 Heidelberg
freitag@mathi.uni-heidelberg.de

Riccardo Salvati Manni
Dipartimento di Matematica,
Piazzale Aldo Moro, 2
I-00185 Roma, Italy.
salvati@mat.uniroma1.it

2013

Introduction

We consider the graded algebra (the generators have weight one)

$$B = \mathbb{Q}[Z_1, Z_2, Z_3, W_1, W_2, W_3, C]$$

with defining relations

$$\begin{aligned} W_1^2 + W_2^2 &= Z_3^2, \\ W_1^2 + W_3^2 &= Z_2^2, \\ W_2^2 + W_3^2 &= Z_1^2, \\ W_1^2 + W_2^2 + W_3^2 &= C^2. \end{aligned}$$

This is a normal graded algebra. The associated projective variety $\operatorname{proj}(B)$ is called the box variety. It is absolutely irreducible. We denote its complexification by

$$\mathcal{B} := \operatorname{proj}(B \otimes_{\mathbb{Q}} \mathbb{C}).$$

It is a surface that characterizes cuboids. The variables W_i give the edges of the cuboid, the variables Z_i the diagonals of the faces and C the long diagonal. We mention that there is an unsolved problem, raised by Euler, whether the box variety contains non-trivial rational points or not. For more details on the box variety we refer to [vL] and [ST].

In this note we describe a parametrization of the box variety (variety of cuboids) by theta functions. This will imply that the box variety is a quotient of the product $\overline{\mathbb{H}/\Gamma[8]} \times \overline{\mathbb{H}/\Gamma[8]}$ of two modular curves of level 8 by a group of order 8 which comes from the diagonal action of $\Gamma[4]$. Actually this parametrization can be defined over the Gauss number field $K = \mathbb{Q}(\mathrm{i})$. We found this parametrization from an observation of D. Testa that the box variety can be embedded into a certain Siegel modular variety which has been described by van Geemen and Nygaard. This background is not necessary for our note and we will not describe it here. But we want to point out that this

still unpublished work of Testa is behind the scenes and we are very grateful that Testa explained to us details of this work.

This parametrization can be used to derive quickly known properties and also some new ones of the box variety. For example, we give in Sect. 2 a modular description of the automorphism group. It can be realized through a subgroup of $\mathrm{SL}(2,\mathbb{Z}) \times \mathrm{SL}(2,\mathbb{Z})$. In [ST], [vL] 140 rational and elliptic curves of the minimal model of the box variety which give generators of the Picard group have been described. We describe them in Sect. 3 in a very simple way as certain modular curves.

In Sect. 3 we consider smooth curves in the box variety. We prove an estimate that shows how their genus grows with their degree. As a consequence, smooth rational and elliptic curves have a bounded degree. This can be considered as validation of a conjecture made in [ST] that the 140 curves described in [vL] exhaust all rational and elliptic curves. This has been proved in [ST] for degrees ≤ 4.

In the paper [Be] of Beauville the box variety arises as a member of a whole family having the same properties, namely to be complete intersections of 4 quadrics in $\mathbb{P}^6$ with an even set of 48 nodes. In this paper Beauville also describes a certain smooth two-fold Galois covering X of the box variety. It is unramified outside the 48 nodes and it is a minimal surface of general type with $q = 4$, $p_g = 7$, $K^2 = 32$. In Sect. 4 we give a very simple modular description of it.

In Sect. 5 a certain involution σ of the box variety $\mathcal{B}$ is considered. We use the modular description to realize the quotient $\mathcal{B}/\sigma$ as a Kummer variety.

In the last section we consider a certain moduli problem which gives the realization of the box variety as fine moduli scheme over $\mathbb{Q}(\mathrm{i})$ classifying pairs (E,F) of elliptic curves with level 4 structures and a compatible isomorphism $E[8] \to F[8]$. This is closely related to work of E. Kani [Ka].

We want to thank A. Beauville, E. Kani and D. Testa for helpful discussions.

1. Generalities about modular groups

We use the standard notations

$$\Gamma[N] = \mathrm{kernel}(\mathrm{SL}(2,\mathbb{Z}) \longrightarrow \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z}))$$

for the principal congruence subgroup of level N of the elliptic modular group and

$$\Gamma_0[N] = \Big\{\, M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z});\ c \equiv 0 \bmod N \,\Big\},$$

$$\Gamma_1[N] = \Big\{\, M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z});\quad a \equiv b \equiv 1 \bmod N,\ c \equiv 0 \bmod N \,\Big\}.$$

We also will use the Igusa groups

$$\Gamma[N,2N] = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \quad ab \equiv cd \equiv 0 \bmod 2N \right\}.$$

In the following we define $\sqrt{a}$ for a non-zero complex number by the principal part of the logarithm. This means that the real part is positive if a is not real and negative and that $\sqrt{a} = \mathrm{i}\,{}_{+}\sqrt{|a|}$ if a is real and negative. Let $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ be a subgroup of finite index and let r be an integral number. By a *multiplier system* of weight $r/2$ one understands a map $v : \Gamma \to S^1$ such that

$$v(M)\sqrt{c\tau + d}^{\,r}, \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

is a cocycle. Then the space $[\Gamma, r/2, v]$ of entire modular forms can be defined in the usual way. Their transformation law is

$$f(M\tau) = v(M)\sqrt{c\tau + d}^{\,r} f(\tau).$$

There are two basic multiplier systems. The theta multiplier system v_ϑ is a multiplier system of weight $1/2$ on the theta group

$$\Gamma_\vartheta := \Gamma[1,2].$$

It can be defined as the multiplier system of the theta function

$$\vartheta(\tau) = \sum_{m=-\infty}^{\infty} e^{\pi \mathrm{i} n^2 \tau}.$$

The theta group is generated by $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. From the theta inversion formula $\vartheta(-1/\tau) = \sqrt{\tau/\mathrm{i}}\vartheta(\tau)$ we get

$$v_\vartheta \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 1, \quad v_\vartheta \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = e^{-\pi \mathrm{i}/4}.$$

We also have to consider the theta function of second kind $\Theta(\tau) := \vartheta(2\tau)$. This is a modular form for $\Gamma_0[4]$. We denote its multiplier system by v_Θ. Both multiplier systems v_ϑ, v_Θ agree on $\Gamma[8]$.

For given Γ, r_0, v we can consider the graded algebra

$$A(\Gamma, r_0, v) := \sum_{r \in \mathbb{Z}} [\Gamma, r r_0, v^r].$$

If it is clear which (r_0, v) has to be considered we will simply write $A(\Gamma)$ for this algebra. This is a finitely generated algebra of Krull dimension 2. The associated projective curve $\mathrm{proj}(A(\Gamma))$ can be identified with

$$\overline{\mathbb{H}/\Gamma} = \mathbb{H}^*/\Gamma \quad \text{where} \quad \mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

We have to consider more generally subgroups of finite index $\Gamma \subset \mathrm{SL}(2,\mathbb{Z}) \times \mathrm{SL}(2,\mathbb{Z})$. A multiplier system v of weight $r/2$ now means a function $v : \Gamma \to S^1$ such that

$$v(M_1, M_2)\sqrt{c_1\tau + d_1}^{\,r}\sqrt{c_2\tau + d_2}^{\,r}$$

is a cocycle. The spaces of modular forms $[\Gamma, r/2, v]$ (now functions of two variables) and the algebras $A(\Gamma) = A(\Gamma, r_0, v)$ are defined in the obvious way.

Let N be a divisor of the natural number N'. In this paper the group

$$\Delta(N, N') = \left\{ (M_1, M_2) \in \Gamma[N] \times \Gamma[N], \quad M_1 \equiv M_2 \bmod N' \right\}$$

will play a role. It is generated by $\Gamma[N'] \times \Gamma[N']$ and the diagonally embedded $\Gamma[N]$.

2. A parametrization of the box variety by theta functions

We make use of the Jacobi theta functions

$$\vartheta_{a,b}(z) = \sum_{n=-\infty}^{\infty} e^{\pi \mathrm{i}(n+a/2)^2 z + b(n+a/2)}.$$

Here (a, b) is one of the three pairs $(0, 0)$, $(1, 0)$, $(0, 1)$. These three functions are modular forms of weight $1/2$ with respect to the three conjugate groups of the theta group. The multiplier systems agree on the group $\Gamma[4, 8]$ with v_ϑ. We also will consider the two theta functions of the second kind $\vartheta_{00}(2\tau)$ and $\vartheta_{10}(2\tau)$. They are modular forms for the two conjugated groups of $\Gamma_0[4]$. Their multiplier systems agree on $\Gamma[2, 4]$ with v_Θ.

So we see that the 5 functions

$$\vartheta_{00}(z), \quad \vartheta_{10}(z), \quad \vartheta_{01}(z), \quad \vartheta_{00}(2z), \quad \vartheta_{10}(2z)$$

have the same multiplier system on $\Gamma[8]$. Hence they are contained in the ring

$$A(\Gamma[8]) := \bigoplus_{r\in\mathbb{Z}} [\Gamma[8], r/2, v_\vartheta^r].$$

It is not difficult to show the following result. The details have been worked out in the Heidelberg Diplomarbeit [Br].

2.1 Theorem. *One has*

$$A(\Gamma[8]) = \mathbb{C}[\vartheta_{00}(z), \vartheta_{10}(z), \vartheta_{01}(z), \vartheta_{00}(2z), \vartheta_{10}(2z)].$$

Defining relations are the classical theta relations

$$\begin{aligned}
\vartheta_{00}(z)^2 &= \vartheta_{00}(2z)^2 + \vartheta_{10}(2z)^2, \\
\vartheta_{01}(z)^2 &= \vartheta_{00}(2z)^2 - \vartheta_{10}(2z)^2, \\
\vartheta_{10}(z)^2 &= 2\vartheta_{00}(2z)\vartheta_{10}(2z).
\end{aligned}$$

Since the multiplier system v_ϑ is defined on the theta group Γ_ϑ, we can define an action of the theta group on $A(\Gamma[8])$ by the formula

$$f|M(\tau) = v_\vartheta(M)^{-r}\sqrt{cz+d}^{-r} f(Mz).$$

This is an action from the right, $f|(M_1M_2) = (f|M_1)|M_2$. We describe it by means of matrices. For this we have to use the action of $\mathrm{GL}(n,\mathbb{C})$ on a complex vector space V with basis $e_1, \dots, e_n$ from the right. It is defined by $Ae_i = \sum a_{ij}e_j$. If we write an element of V in the form $\sum x_ie_i$ then this means that the row $x = (x_1, \dots, x_n)$ had to be multiplied from the right by the matrix A. Standard theta transformation formulas give the following result.

2.2 Lemma. *The matrix* $\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)$ *acts with respect to the basis*

$$\vartheta_{00}(z), \quad \vartheta_{10}(z), \quad \vartheta_{01}(z), \quad \vartheta_{00}(2z), \quad \vartheta_{10}(2z)$$

through the diagonal matrix with the diagonal entries

$$1, \mathrm{i}, 1, 1, -1.$$

The matrix $\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ *acts with respect to this basis through the matrix*

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\
0 & 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2}
\end{pmatrix}$$

We are interested in the action of $\Gamma[4]$ on $A(\Gamma[8])$. The factor group $\Gamma[4]/\Gamma[8]$ is ismorphic to $\mathbb{Z}/2\mathbb{Z}^3$. It is generated by the images of the matrices

$$T = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \quad T' = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix}.$$

From Lemma 2.2 we get the following result.

2.3 Lemma. *The generators T, T', R of $\Gamma[4]/\Gamma[8]$ act on $A(\Gamma[4])$ by means of the diagonal matrices*

$$\begin{aligned} T &\longmapsto \operatorname{diag}(1,-1,1,1,1), \\ T' &\longmapsto \operatorname{diag}(1,1,-1,,1,1), \\ R &\longmapsto \operatorname{diag}(1,1,1,-1,-1). \end{aligned}$$

Now we consider modular forms of two variables. We consider the ring $A(\Gamma[8]\times\Gamma[8])$ of modular forms of integral or half integral weight $r/2$ with respect to the multiplier system $(v_\vartheta(M_1)v_\vartheta(M_2))^r$. It is clear that

$$A(\Gamma[8]\times\Gamma[8]) := \mathbb{C}[f(z)g(w)], \quad f,g \in \{\vartheta_{00}(\cdot),\vartheta_{10}(\cdot),\vartheta_{01}(\cdot),\vartheta_{00}(2\cdot),\vartheta_{10}(2\cdot)\}.$$

We want to determine the subring $A(\Delta(4,8))$ of modular forms with respect to the group $\Delta(4,8)$. This is the ring of invariants with respect to the diagonal action of $\Gamma[4]$ by means of the action

$$f(z,w) \longmapsto v_\vartheta(M)^{-2r}\sqrt{cz+d}^{\,-r}\sqrt{cw+d}^{\,-r} f(Mz,Mw).$$

Using Lemma 2.3 it is obvious that the forms

$$\begin{aligned} &\vartheta_{00}(z)\vartheta_{00}(w), \\ &\vartheta_{10}(z)\vartheta_{10}(w), \\ &\vartheta_{01}(z)\vartheta_{01}(w), \\ &\vartheta_{00}(2z)\vartheta_{00}(2w), \\ &\vartheta_{00}(2z)\vartheta_{10}(2w), \\ &\vartheta_{10}(2z)\vartheta_{00}(2w), \\ &\vartheta_{10}(2z)\vartheta_{10}(2w). \end{aligned}$$

are invariant under $\Gamma[4]$. Moreover, one can show that they generate the invariant ring.

2.4 Theorem. *There is an isomorphism*

$$B\otimes_{\mathbb{Q}}\mathbb{C} \xrightarrow{\sim} A(\Delta(4,8))$$

which is given by

$$\begin{aligned} Z_1 &\longmapsto \vartheta_{01}(z)\vartheta_{01}(w), \\ Z_2 &\longmapsto \vartheta_{00}(z)\vartheta_{00}(w), \\ Z_3 &\longmapsto \vartheta_{10}(z)\vartheta_{10}(w), \\ C &\longmapsto \vartheta_{00}(2z)\vartheta_{00}(2w)+\vartheta_{10}(2z)\vartheta_{10}(2w), \\ W_1 &\longmapsto \vartheta_{10}(2z)\vartheta_{00}(2w)+\vartheta_{00}(2z)\vartheta_{10}(2w), \\ W_2 &\longmapsto \mathrm{i}(\vartheta_{10}(2z)\vartheta_{00}(2w)-\vartheta_{00}(2z)\vartheta_{10}(2w)), \\ W_3 &\longmapsto \vartheta_{00}(2z)\vartheta_{00}(2w)-\vartheta_{10}(2z)\vartheta_{10}(2w). \end{aligned}$$

Hence we have $\mathcal{B}\cong\overline{\mathbb{H}\times\mathbb{H}/\Delta(4,8)}$.

Proof. Classical theta relations

$$\begin{aligned}\vartheta_{00}(z)^2 &= \vartheta_{00}(2z)^2 + \vartheta_{10}(2z)^2,\\ \vartheta_{01}(z)^2 &= \vartheta_{00}(2z)^2 - \vartheta_{10}(2z)^2,\\ \vartheta_{10}(z)^2 &= 2\vartheta_{00}(2z)\vartheta_{10}(2z).\end{aligned}$$

show that this is a homomorphism. Obviously it is surjective. Since $A(\Delta(4,8))$ is an integral domain of Krull dimension three and since B also has dimension three, this homomorphism must be an isomorphism. □

The modular picture can be used to recover known properties of the box variety. We mention some of them.

First we describe the automorphism group of the box variety. The group $\Delta(4,8)$ is a normal subgroup of $\Delta(1,2)$. The index is 768. Hence the quotient $\Delta(1,2)/\Delta(4,8)$ is a subgroup of order 768 of the automorphism group. The involution $(z,w)\mapsto(w,z)$ gives an extra automorphism. Both together generate a subgroup of order 1 536 of the automorphism group. Due to [ST] the order of the automorphism group is 1 536. Hence we described the full automorphism group.

Now we describe the singularities. It is known that the box variety has 48 singularities which all are nodes. In the modular picture they correspond to some zero dimensional cusps. These are the images of the points (a,b) where $a,b\in\mathbb{Q}\cup\{\infty\}$. There are two types of such points. It may happen that (a,b) is the fixed point of pair (M_1,M_2) of parabolic elements. The typical case is (∞,∞) and $A=B=\left(\begin{smallmatrix}1&4\\0&1\end{smallmatrix}\right)$. The group $\Delta(1,2)$ acts transitively on them. There are pairs which do not have this property. The precise picture is as follows.

2.5 Proposition. *The box variety $\overline{\mathbb{H}\times\mathbb{H}/\Delta(4,8)}$ contains* 96 *zero dimensional cusps. They decompose into two orbits of* 48 *cusps under* $\Delta(1,2)$. *The orbit containing the image of* (∞,∞) *defines the singular locus.*

A slightly different way to see this is to consider the Galois coverings

$$\overline{\mathbb{H}/\Gamma[8]}\times\overline{\mathbb{H}/\Gamma[8]}\longrightarrow\overline{\mathbb{H}\times\mathbb{H}/\Delta(4,8)}\longrightarrow\overline{\mathbb{H}/\Gamma[2]}\times\overline{\mathbb{H}/\Gamma[2]}.$$

The covering group of the first cover is $G=\Delta(4,8)/\Gamma[8]\times\Gamma[8]\cong(\mathbb{Z}/2\mathbb{Z})^3$. The singular points of the box variety are the images of the fixed points of G. They agree with the fibres of three zero dimensional cusps of $\overline{\mathbb{H}/\Gamma[2]}\times\overline{\mathbb{H}/\Gamma[2]}$ which are of the form (a,a). Thy can be represented by (∞,∞), $(0,0)$ and $(1,1)$. In the typical case (∞,∞) one can take $p=e^{2\pi\mathrm{i}z/8}$, $q=e^{2\pi\mathrm{i}w/8}$ as uniformizing parameters of $\overline{\mathbb{H}/\Gamma[8]}\times\overline{\mathbb{H}/\Gamma[8]}$. The stabilizer in G is generated by the translation $(z,w)\mapsto(z+4,w+4)$ wich acts by $(p,q)\mapsto-(p,q)$. Hence the singularity appears as quotient singularity of the type $(\mathbb{C}\times\mathbb{C})/\pm$ which actually is a node.

We denote by $\tilde{\mathcal{B}}$ the minimal resolution of the 48 nodes. The exceptional divisor is the union of 48 lines.

Next we describe the holomorphic differential forms on $\tilde{\mathcal{B}}$. The modular curve $\overline{\mathbb{H}/\Gamma[8]}$ has genus 5. The differentials

$$\begin{aligned}
\omega_1(z) &= \vartheta_{00}(z)^2\vartheta_{01}(z)\vartheta_{10}(z)dz,\\
\omega_2(z) &= \vartheta_{00}(z)\vartheta_{01}(z)^2\vartheta_{10}(z)dz,\\
\omega_3(z) &= \vartheta_{00}(z)\vartheta_{01}(z)\vartheta_{10}(z)^2dz.\\
\omega_4(z) &= \vartheta_{00}(2z)\vartheta_{00}(z)\vartheta_{01}(z)\vartheta_{10}(z)dz.\\
\omega_5(z) &= \vartheta_{10}(2z)\vartheta_{00}(z)\vartheta_{01}(z)\vartheta_{10}(z)dz.
\end{aligned}$$

are holomorphic on $\overline{\mathbb{H}/\Gamma[8]}$, since the defining modular forms are cusp forms. A simple computation gives that

$\psi_1 = \omega_1(z)\wedge\omega_1(w),\ \psi_2 = \omega_2(z)\wedge\omega_2(w),\ \psi_3 = \omega_3(z)\wedge\omega_3(w),\ \psi_4 = \omega_4(z)\wedge\omega_4(w),\ \psi_5 = \omega_4(z)\wedge\omega_5(w),\ \psi_6 = \omega_5(z)\wedge\omega_4(w),\ \psi_7 = \omega_5(z)\wedge\omega_5(w)$

are $\Delta(4,8)$-invariant holomorphic differential forms. One can check that they extend holomorphically to the desingularization $\tilde{\mathcal{B}}$. In this way one can recover the result of [ST] that the minimal resolution of the box variety has geometric genus 7. One can also derive from this picture that the box variety is of general type.

In the paper [ST] the structure of the Picard group of $\tilde{\mathcal{B}}$ has been determined. It is a free abelian group of rank 64. Stoll and Testa proved that certain 140 curves defined already in [vL] generate this group. There are 80 rational and 60 elliptic curves. We first describe the rational curves. The 48 exceptional curves belong to them. The remaining 32 rational curves have the following easy modular description.

2.6 Proposition. *The equations $w = Mz + k$ where M runs through a system of representatives of $\Gamma[4]/\Gamma[8]$ and $k \in \{0,2,4,6\}$ define 32 smooth rational curves in the box variety. There union is the zero set of the modular form*

$$\vartheta_{00}(z)^4\vartheta_{01}(w)^4 - \vartheta_{01}(z)^4\vartheta_{00}(w)^4 \qquad (= 4\mathrm{i}W_1W_2W_3C).$$

Next we describe the elliptic curves. Part of them is in the Satake boundary. The Satake boundary is the union of the images of $\mathbb{H}^*\cup\{a\}$ and $\{a\}\cup\mathbb{H}^*$, where $a\in\mathbb{Q}\cup\{\infty\}$. It is easy to work out the structure.

2.7 Proposition. *The Satake boundary consists of 12 (smooth) elliptic curves. Each of them contains 8 singular and 8 smooth zero dimensional cusps. The whole Satake boundary is the zero set of the modular form*

$$\vartheta_{00}(z)\vartheta_{10}(z)\vartheta_{01}(z)\vartheta_{00}(w)\vartheta_{10}(w)\vartheta_{01}(w) \qquad (= Z_1Z_2Z_3).$$

We will not give the details of the proof but we explain a typical boundary curve. We take the image of $\mathbb{H}^* \times \{\infty\}$. This is the modular curve with respect to the group $\Gamma_1[8] \cap \Gamma[4]$. It contains $\Gamma[8]$ as a subgroup of index 2. It is not difficult to work out the structure of the ring of modular forms. Details can be found in [Kl].

2.8 Proposition. *The ring $A(\Gamma_1[8] \cap \Gamma[4])$ of all modular forms of half integral weight for the group $\Gamma_1[8] \cap \Gamma[4]$ with respect to the multiplier system v_ϑ^r is generated by*

$$a = \vartheta_{0,0}(z), \quad b = \vartheta_{0,1}(z), \quad c = \vartheta_{0,0}(2z), \quad d = \vartheta_{1,0}(2z).$$

Defining relations are

$$a^2 = c^2 + d^2, \quad b^2 = c^2 - d^2.$$

This is an intersection of two quadrics in $\mathbb{P}^3$ and hence an elliptic curve. So this describes one of the 12 elliptic curves in the boundary part of the box variety.

Finally we describe the 48 elliptic curves that are not contained in the boundary.

2.9 Proposition. *The equation $w = z + 1$ describes an elliptic curve in the box variety which also can be defined by the equations*

$$W_1 = W_2,\ Z_1 = Z_2,\ \sqrt{2}W_1 = Z_3,\ W_3^2 + Z_3^2 - C^2 = 0,\ 2Z_2^2 + Z_3^2 - 2C^2 = 0.$$

Applying the group $\Delta(1,2)$ one gets 48 elliptic curves.

3. Curves in the box variety

We want to study irreducible curves $C \subset \mathcal{B}$ in the box variety. We have to make the rather strong assumption that the normalization map $\bar{C} \to C$ is bijective. We denote by g the genus of $\bar{C}$. We use the following fact which has been explained in [ST] and [Be] and which can be seen from the explicit description of the holomorphic 2-forms on $\tilde{\mathcal{B}}$ above: the canonical map (defined by the canonical divisor on $\tilde{\mathcal{B}}$) is the composition of the natural projection $\tilde{\mathcal{B}} \to \mathcal{B}$ and the original embedding $\mathcal{B} \to \mathbb{P}^6$. This shows the that the degree d of C in $\mathbb{P}^6$ equals the intersection number of the strict transform of C in $\tilde{\mathcal{B}}$ and a canonical divisor on $\tilde{\mathcal{B}}$.

3.1 Theorem. *Let $C \subset \mathcal{B}$ be a curve such that the normalization map $\bar{C} \to C$ is bijective. Let g be the genus of $\bar{C}$ and d be the degree of C. Then the inequality*

$$d \leq 176 + 16g$$

holds.

As a consequence, rational end elliptic curves have bounded degree. This supports a conjecture in [ST] that each rational or elliptic curve in $\tilde{\mathcal{B}}$ belongs to the system of 140 curves described above.

Proof of Theorem 3.1. Let k be a natural number. We consider a modular form of weight $4k$ for the group $\Delta(4,8)$. Then we consider the tensor

$$T = \Delta(z)^k \Delta(w)^k f(z,w)(dzdw)^{8k}$$

in the algebra of symmetric tensors. Since the modular form Δ has weight 12, this tensor is invariant under $\Delta(4,8)$. Hence it defines a meromorphic tensor on $\tilde{\mathcal{B}}$. Using the coordinates $p = e^{2\pi \mathrm{i} z/8}$, $q = e^{2\pi \mathrm{i} w/8}$, it is easy to check that this tensor is holomorphic outside the 48 exceptional curves. In the exceptional curves it may have poles. We can lift the curve $\bar{C}$ to a holomorphic map $\varphi : \bar{C} \to \tilde{\mathcal{B}}$. Then we consider the pulled back tensor $\varphi^* T$. This is a meromorphic tensor of degree $16k$ on $\bar{C}$.

We can assume that C is not the image of a $\mathbb{H}^* \times \{a\}$ or $\{a\} \times \mathbb{H}^*$ for an $a \in \mathbb{H}^*$, since for these curves the theorem can be seen directly. Then the tensor $\varphi^* T$ vanishes if and only f vanishes along C as a function. Since the weight k can be made large we can choose f that it doesn't vanish along C and in addition we can get that f does not vanish at any of the 48 nodes in $\mathcal{B}$.

We assume that C contains one the nodes, for example the image of the cusp (∞, ∞). Then we can consider a parametrization of the curve close to this cusp. A simple lemma (compare [Fr], Satz 1) shows that the curve can be parametrized by a holomorphic map $\alpha : \mathbb{H} \to \mathbb{H} \times \mathbb{H}$ as follows:

$$\alpha(z) = z(a_1, a_2) + (\Phi_1(q), \Phi_2(q)), \quad q = e^{2\pi \mathrm{i} \tau},$$

where Φ_i are holomorphic at $q = 0$. The pair (a_1, a_2) is contained in the translation lattice, i.e.

$$a_1 \equiv a_2 \equiv 0 \mod 4, \quad a_1 + a_2 \equiv 0 \mod 8.$$

The numbers a_1, a_2 are both positive. This implies $a_1 + a_2 \geq 8$.

We study the poles and zeros of the tensor $\varphi^* T$. Since its divisor is the $16k$-multiple of a canonical divisor, we have

$$16(2g-2)k = \#\text{zeros} - \#\text{poles}.$$

First we estimate the number of poles of φ^*T from above (counted with multiplicity). The poles are intersection points of $\bar{C}$ with the exceptional divisor. Since $\bar{C} \to C$ is bijective, $\bar{C}$ can meet each of the 48 exceptional curves at most once. Hence the set of poles contains at most 48 points.

We have to estimate the pole order. It is sufficient to do this for the standard node, i.e. the image of the cusp (∞, ∞) and we can do this by means of the curve lemma. The term $(dzdw)^{8k}$ contributes with $16k$ to the pole order and $\Delta(z)\Delta(w)$ contributes with a zero of order $(a_1 + a_2)k \geq 8k$. Hence the pole order of the tensor at the node is at most $8k$. Since we have 48 nodes the total pole order is estimated by $384k$.

Next we estimate the number of zeros from below. Each intersection point of the zero divisor of f with the curve produces a zero. (Since we assumed that f doesn't vanish at the nodes, there is no conflict with the poles of T.) Since the zero divisor of f is a $2k$-multiple of the canonical divisor, we get that there are at least $2kd$ zeros. So we get

$$16(2g-2)k = \#\text{zeros} - \#\text{poles} \geq 2kd - 384k.$$

This finishes the proof of Theorem 3.1. $\square$

Remark. As we mentioned the tensor $T = \Delta(z)^k \Delta(w)^k f(z,w)(dzdw)^{8k}$ can have poles along the 48 exceptional divisors. The results of Theorem 3.1 could be improved if one could find f such that T is holomorphic on the the whole $\tilde{\mathcal{B}}$. We did not succeed to find such f and we think that they don't exist. But we could not prove this.

4. A two-fold covering of the box variety

We consider the subgroup $\Gamma'[4]$ of index two of $\Gamma[4]$ which is defined by

$$a + b + c \equiv 1 \mod 8.$$

4.1 Lemma. *The group $\Gamma'[4]/\Gamma[8]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It acts freely on $\overline{\mathbb{H}/\Gamma[8]}$.*

Proof. Let b by a point of the extended upper half plane $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. Assume that $M \in \Gamma'[4] - \Gamma[8]$ is a matrix that fixes a mod $\Gamma[8]$. Then there exists an element $A \in \Gamma[8]$ such that $M(a) = A(a)$. The matrix $N = A^{-1}M$ then fixes a. This matrix is also contained in $\Gamma'[4]$ and not in $\Gamma[8]$. Modulo 8 it is one of the following three

$$\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, \quad \begin{pmatrix} 5 & 4 \\ 0 & 5 \end{pmatrix}, \quad \begin{pmatrix} 5 & 0 \\ 4 & 5 \end{pmatrix}.$$

Since it has a fixed point, the absolute value of its trace is bounded by 2. We treat the three cases separately. In the first case we have

$$N = \begin{pmatrix} 1+8\alpha & 4+8\beta \\ 4+8\gamma & 1+8\delta \end{pmatrix}.$$

The condition for the trace implies $\delta = -\alpha$. The determinant is 1. But the condition $\delta = -\alpha$ implies that the determinant is $1 - 16 \bmod 32$. This is a contraction.

In the second case we have

$$N = \begin{pmatrix} 5+8\alpha & 4+8\beta \\ 8\gamma & 5+8\delta \end{pmatrix}.$$

The condition for the trace now gives $\delta = -\alpha - 1$. Now the determinant would be congruent 4 mod 8 which is not possible. The same argument works in the third case. □

We consider the (non-singular) manifold

$$X := \overline{\mathbb{H}/\Gamma[8]} \times \overline{\mathbb{H}/\Gamma[8]}/\Gamma'[4]$$

where $\Gamma'[4]$ acts diagonally. The inclusion $\Gamma'[4] \hookrightarrow \Gamma[4]$ gives a two fold covering $X \to \mathcal{B}$ of the box variety. Locally around the 48 singularities of $\mathcal{B}$ this looks like the covering $\mathbb{C}^2 \to \mathbb{C}^2/\pm$. One can desingularize the node at 0 be first blowing up the origin in the covering $\mathbb{C}^2$. The involution $(z, w) \mapsto (-z, -w)$ lifts to this resolution and the quotient is smooth. The same can be done globally. We blow up X at the 48 inverse images of the nodes of $\mathcal{B}$. This gives a manifold $\tilde{X}$. The Galois involution of X over $\mathcal{B}$ lifts to $\tilde{X}$ and the quotient $\tilde{\mathcal{B}}$ is just the blow up of $\mathcal{B}$ at the nodes. So we have a commutative diagram

$$\begin{array}{ccc} \tilde{X} & \longrightarrow & \tilde{\mathcal{B}} \\ \downarrow & & \downarrow \\ X & \longrightarrow & \mathcal{B} \end{array}.$$

The map $\tilde{X} \to \tilde{\mathcal{B}}$ is ramified along the exceptional divisors (48 lines). The existence of this covering and its uniqueness have been treated in the paper [Be]. We call

$$X = \overline{\mathbb{H}/\Gamma[8]} \times \overline{\mathbb{H}/\Gamma[8]}/\Gamma'[4]$$

the Beauville manifold. The existence of X is equivalent to the fact that the exceptional divisor is divisible by two in the Picard group $\mathrm{Pic}(\tilde{\mathcal{B}})$. The uniqueness follows from the fact that this Picard group is torsion free [ST]. We refer to [Be] for more interesting properties of the surface X. Some of them can be easily derived form the modular picture.

Since X has the product of two curves of genus > 1 as unramified covering, the universal covering of X is the product $\mathbb{E} \times \mathbb{E}$ of two unit disks. Let C

be the Riemann sphere or a torus $\mathbb{C}/L$ and let $\alpha : C \to X$ be a holomorphic map. This map lifts to the universal coverings. Since every holomorphic map $\mathbb{C} \to \mathbb{E}$ is constant, we obtain that α is constant. Hence X contains no rational or elliptic curve. This argument applies also to the regular locus $\mathcal{B}_{\text{reg}}$ of the box variety, since its universal covering is the complement of a discrete subset in $\mathbb{E} \times \mathbb{E}$. Hence we obtain the following result.

4.2 Remark. *Every rational or elliptic curve in the boy variety contains at least one node.*

5. Relation to a Kummer variety

In this section we consider the $\mathbb{Q}$-structure of the box variety. It is the associated projective variety of the algebra

$$B = \mathbb{Q}[W_1, W_2, W_3, Z_1, Z_2, Z_3, C]$$

(with the defining relations of the box variety). We consider the involution $\sigma(Z_3) = -Z_3$ of the ring B. It induces an involution of the box variety. The invariant ring is

$$B^\sigma = \mathbb{Q}[Z_1, Z_2, C, W_1, W_2, W_3]$$

with defining relations

$$\begin{aligned} W_1^2 + W_3^2 &= Z_2^2, \\ W_2^2 + W_3^2 &= Z_1^2, \\ W_1^2 + W_2^2 + W_3^2 &= C^2. \end{aligned}$$

The associated projective variety is the quotient of the box variety by σ. This is a also a modular variety, since in the picture of Theorem 2.4 transformation σ is induced by the modular substitution

$$(z, w) \longmapsto (Tz, w).$$

This gives the following result.

5.1 Lemma. *The variety $\mathcal{B}/\sigma$ is defined over $\mathbb{Q}$. Over $\mathbb{C}$ it agrees with the modular variety which belongs to the subgroup of $\mathrm{SL}(2,\mathbb{Z}) \times \mathrm{SL}(2,\mathbb{Z})$ that is generated by $\Gamma[8] \times \Gamma[8]$ and the elements*

$$(T, E), \quad (E, T), \quad (T', T'), \quad (R, R).$$

We considered already in Proposition 2.8 the group $\Gamma_1[8]\cap\Gamma[4]$ and explained the structure of the ring of modular forms. We defined 4 generators a,b,c,d with defining relations

$$a^2=c^2+d^2,\quad b^2=c^2-d^2.$$

Since these relations are defined over $\mathbb{Q}$, we can can consider this algebra over $\mathbb{Q}$

$$A(\Gamma_1[8]\cap\Gamma[4])=C\otimes_{\mathbb{Q}}\mathbb{C},\quad C:=\mathbb{Q}[a,b,c,d].$$

and obtain an elliptic curve E over $\mathbb{Q}$. One can compute its normal form over $\mathbb{Q}$:

$$y^2=x^3-x.$$

Its projective form is $y^2z=x^3-xz^2$. An explicit isomorphism is given by

$$x=a-b,\quad y=2d,\quad z=2c-a-b.$$

We consider the automorphisms

$$\tau(a,b,c,d)=(a,-b,c,d),\quad \rho(a,b,c,d)=(a,b,-c,-d)$$

of the algebra.

They correspond to the modular transformations T' and R whereas T acts as identity. The two transformations generate a group $H\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

5.2 Lemma. *The transformation ρ is an involution without fixed point of the elliptic curve E. Hence it is a translation by a two-torsion point. The transformation τ is an involution with the fixed point $[\sqrt{2},0,1,1]$. Hence the following is true. If one considers E as an elliptic curve over $\mathbb{Q}(\sqrt{2})$ with origin $[\sqrt{2},0,1,1]$ then τ corresponds to the negation $x\mapsto -x$.*

We want to consider the product of two copies of this curve. This is the projective variety associated with the graded algebra

$$C_2=\mathbb{Q}[a\otimes a,a\otimes b,\dots,d\otimes d].$$

In the modular picture we have to identify

$$a\otimes a=\vartheta_{00}(z)\vartheta_{00}(w),\dots,d\otimes d=\vartheta_{10}(2z)\vartheta_{10}(2w).$$

The group H acts diagonally on C_2. The fixed ring is just B^σ. Hence we get the following result.

5.3 Proposition. *There is a biholomorphic map*

$$(E \times E)/H \xrightarrow{\sim} \mathcal{B}/\sigma,$$

defined over the field of Gauss numbers.

The variety $(E \times E)/H$ can be understood as follows. We first take the quotient by the translation ϱ. This gives an abelian variety over $\mathbb{Q}$.

$$X = (E \times E)/\varrho.$$

Then we take the quotient by τ. If we extend the base field $\mathbb{Q}$ by $\sqrt{2}$, and take $[\sqrt{2}, 0, 1, 1]$ diagonally embedded as origin then τ corresponds to the negation and

$$(E \times E)/H = X/\pm$$

appears as a Kummer variety. Hence over the field $\mathbb{Q}(\mathrm{i}, \sqrt{2})$ of eighth roots of unity, the variety $\mathcal{B}/\sigma$ can be identified with a Kummer variety.

6. A moduli problem

We denote by (Sch/S) the category of schemes over a base scheme S. For $S = \mathrm{Spec}(A)$ we write (Sch/A). We fix an algebraic number field K. We also fix an embedding $K \hookrightarrow \mathbb{C}$. Let E be an elliptic curve over a scheme $S \in (\mathrm{Sch}/K)$ and N a natural number. We denote by $E[N]$ the kernel of multiplication by N from E to E. This is a group scheme over S. If T as a scheme over S then the T-valued points are

$$E[N](T) = \mathrm{kernel}(E(T) \xrightarrow{\cdot N} E(T)).$$

To each finite group G there is associated a group scheme which we denote by the same letter and which is defined by $G(S) = G$ for connected S. We call it the constant group scheme associated to G. It may be that $E[N](S)$ is isomorphic $(\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z})(S)$. A level N structure on E then means the choice of an isomorphism $(\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z})(S) \xrightarrow{\sim} E[N](S)$. It extends to an ismorphism of $E(N)$ to the constant group scheme associated to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

We denote by G_m the group scheme "multiplicative group" over K. It is defined by $G_m(S) = \mathcal{O}(S)^*$ (multiplicative group). The kernel of powering by N is the group scheme μ_N. Hence

$$\mu_N(S) = \{a \in \mathcal{O}(S);\ a^N = 1\}.$$

For an elliptic curve E over $S \in (\mathrm{Sch}/K)$ there exists the Weil-pairing. It associates to each S-scheme T an alternating map

$$E[N](T) \times E[N](T) \longrightarrow \mu_N(T).$$

When K contains the cyclotomic field of N-th roots of unity, then μ_N is the constant group scheme associated to the abstract group

$$\mu_N = \{\zeta \in \mathbb{C};\ \zeta^N = 1\} \cong \mathbb{Z}/N\mathbb{Z}.$$

We also can consider the symplectic pairing

$$e_N : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \longrightarrow \mu_N, \quad e((a_1, a_2), (b_1, b_2)) = e^{2\pi \mathrm{i}(a_1 b_2 - a_2 b_1)/N}.$$

From now on we assume that K contains the Nth roots of unity. Since we consider a fixed embedding of K into $\mathbb{C}$, we can identify μ_N and $\mu_N(K)$. So it makes sense to consider level N-structures which preserve the symplectic pairings and we will use the notion "Level N-structure" from now on in this restricted sense.

We want to formulate a moduli problem. For this we introduce the category (Ell2) (compare [Ka]). Its objects are pairs of elliptic curves $E \to S$, $F \to S$ over a variable scheme $S \in \mathrm{Sch}/K$. Morphisms are pairs of cartesian squares

$$\begin{array}{ccccccc} E_1 & \longrightarrow & E & \qquad & F_1 & \longrightarrow & F \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ S_1 & \longrightarrow & S & & S_1 & \longrightarrow & S \end{array}$$

This category is a gruppoid, i.e. all morphims are isomorphisms. A moduli problem on (Ell2) is a functor $\mathcal{P}$ from (Ell2) into the category of sets. It is called representable if there exists a universal $\mathbf{E} \to \mathcal{M}(\mathcal{P})$ in the sense that there is a functorial ismorphism

$$\mathcal{P}(E/S) = \mathrm{Hom}_{(\mathrm{Ell2})}(E/S, \mathbf{E}/\mathcal{M}(\mathcal{P})).$$

We recall that the moduli problem $\mathcal{P}$ is called *relatively representable* if for every $(E, F)/S$ in (Ell2) the functor on (Sch/S) that associates to a scheme T/S the set $\mathcal{P}((E_T, F_T)/T)$ is representable by some scheme $\mathcal{P}_{E/S}$.

Every representable moduli problem is also relatively representable. Let $\mathcal{P}'$ and $\mathcal{P}''$ two moduli problems. Then one can define the simultaneous moduli problem $\mathcal{P} = (\mathcal{P}', \mathcal{P}'')$ in the obvious way. Assume that $\mathcal{P}'$ is representatable and $\mathcal{P}''$ is relatively representable. Then it is easy to see that $\mathcal{P}$ is representable.

We now consider two natural numbers $N|N'$. We recall that we assume that K containes the Nth roots of unity. We define a moduli problem $\mathcal{P}(N, N')$. It associates to $(E, F)/S$ the set of pairs (α, β)

$$\alpha : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \stackrel{\sim}{\longrightarrow} E[N], \quad \beta : E[N'] \stackrel{\sim}{\longrightarrow} F[N'].$$

Here α is a level N-structure (preserving the Weil-pairing) and β is an isomorphism of S-groups, also preserving Weil-pairings. We notice that α and β induce a level N-structure of F.

6.1 Theorem. *Assume $N \geq 3$. The moduli problem $\mathcal{P}(N,N')$ is representable.*

Proof. The moduli problem $\mathcal{P} = \mathcal{P}(N,N')$ can be considered as a simultaneous problem $(\mathcal{P}', \mathcal{P}'')$. Here $\mathcal{P}'$ refers to the level 4 moduli problem and $\mathcal{P}''$ associates to $(E,F)/S$ the set of isomorphisms $E[N'] \to F[N']$ (preserving the Weil pairing). It is known that $\mathcal{P}'$ is representable. Hence it remains to show that $\mathcal{P}''$ is locally representable. For this we have to fix a pair of elliptic curves $E \to S$, $F \to S$ over a scheme $S \in (\mathrm{Sch}/K)$. Then we have to consider the functor on the category of schemes over S that associates to an scheme T over S the set of isomorphisms $E_T[N'] \to F_T[N']$. It is well-known that this functor is representable and also the subfunctor preserving the Weil pairing is representable. □

We denote the moduli space of the functor $\mathcal{P}(N,N')$ by $\mathcal{M}(N,N')$. This is an affine algebraic variety over $\mathbb{Q}(\mathrm{i})$. Over $\mathbb{C}$ it is $\mathbb{H} \times \mathbb{H}/\Delta(N,N')$.

We are interested in the group $\Delta(4,8)$. Theorem 2.4 says that the surface $\mathbb{H} \times \mathbb{H}/\Delta(4,8)$ is embedded as an open part of the box variety. We call this the *finite part of the box variety.* We have now two K-structures, one coming form the defining equations of the box variety and the other coming form the moduli problem $\mathcal{M}(4,8)$. A variant of the q-expansion principle shows that both are the same. Hence we get the following result.

6.2 Theorem. *The variety $\mathcal{M}(4,8)$ is isomorphic as variety over $\mathbb{Q}(\mathrm{i})$ to the finite part of the box variety (considered as variety over $\mathbb{Q}(\mathrm{i})$).*

This gives us a description of $\mathbb{Q}(\mathrm{i})$-rational points of the box variety in terms of elliptic curves.

6.3 Theorem. *The $\mathbb{Q}(\mathrm{i})$-valued points of the finite part of the box variety are in one-to-one correspondence to isomorphy classes of pairs of elliptic curves E, F over $\mathbb{Q}(\mathrm{i})$, equipped with a level 4 structure of E and a compatible isomorphism of group schemes $E[8] \to F[8]$ which preserves the Weil pairing.*

References

[Be] Beauville, A.: *A tale of two surfaces,*, http://arxiv.org/abs/1303.1910

[Br] Brieger, S.: *Modulformen zur Stufe 8*, Diplomarbeit, Universität Heidelberg (2010)

[Fr] Freitag, E.: *Eine Bemerkung zur Theorie der Hilbertschen Modulmannigfaltigkeiten hoher Stufe,* Math. Z. **171**, 27–38 (1980)

[Ka] Kani, E.: *Mazur's question and modular diagonal quotient surfaces,* preprint (2011)

[Kl] Klein, M.: *Ein Ring von Modulformen zur Stufe 8*, Diplomarbeit, Universität Heidelberg (2011)

[vL] van Luijk, R.: *On perfect cuboids,* Undergraduate thesis, University Utrecht (2000)

[ST] Stoll, M., Testa, D.: *The surface parametrizing cuboids*
preprint arXiv: 1009.0388